ISTITUTO COMPRENSIVO POLLINA - SAN MAURO CASTELVERDE
VIA LEONARDO SCIASCIA - FINALE 90010 POLLINA (PA)
Tel 0921426567 - Fax 0921426567
Codice Meccanografico: PAIC818003 - Codice Fiscale: 82000690824
PEO: paic818003@istruzione.it *PEC:* paic818003@pec.istruzione.it *Sito Web:* www.icpollinasanmaurocastelverde.edu.it

SMART WORKING E PROTEZIONE DEI DATI PERSONALI

Indicazioni operative per un corretto trattamento di dati personali nel contesto dello "smart working"

Il lavoratore è tenuto ad applicare le misure di sicurezza informatica e salvaguardare i dati secondo i principi stabiliti dal D.Lgs. 196/2003, dal D.Lgs. 101/2018 e ss.mm.ii. contenente il "Codice in materia di protezione dei dati personali".

Il lavoratore è tenuto al rispetto del Codice di comportamento dei lavoratori pubblici e il Codice disciplinare di cui al Titolo III del CCNL 2019-2021, a prestare la sua attività con diligenza, ad assicurare assoluta riservatezza sul lavoro affidatogli e su tutte le informazioni contenute nelle banche dati e ad attenersi alle istruzioni ricevute dal dirigente scolastico e dal direttore SGA relativamente all'esecuzione del lavoro.

Misure che il dipendente in smart working deve applicare

Si fornisce una serie di indicazioni operative per il trattamento e la sicurezza dei dati personali nel contesto dello "smart working" dettati dall'esigenza di regolamentare modalità lavorativee garantire la riservatezza dei dati:

- i dipendenti devono svolgere i trattamenti previsti dalle rispettive mansioni nel rispetto delle prescrizioni e indicazioni operative contenute negli atti di individuazione quali persone autorizzate al trattamento, ai sensi dell'art. 29 del RGPD ("Regolamento Generale sulla Protezione dei Dati").

- indipendentemente dalle diverse concrete vie di implementazione dello "smart working", avendo necessariamente a che fare con dispositivi informatici, è necessario che il lavoratore garantisca un adeguato livello di protezione di tali dispositivi, attenzionando in particolare il rispetto dei principi di integrità, riservatezza e disponibilità dei dati e delle informazioni ivi contenute, al fine di ridurre al minimo i rischi di accesso non autorizzato, di trattamento non consentito o non conforme alle finalità oppure di distruzione o perdita dei dati stessi. A tale scopo occorre:

  1. proteggere l'accesso ai dispositivi informatici (computer, tablet, smartphone) e delle connessioni (cablate o Wi-Fi) attraverso l'uso di password sufficientemente robuste e sicure: a tal proposito si consiglia di utilizzare password lunghe in quanto più difficili da scoprire e prive di riferimenti ai dati anagrafici propri e dei familiari; ciò vale tanto per l'accesso ai propri dispositivi quanto per l'accesso a Internet, in quanto la diffusa prassi di non cambiare la password di default per l'accesso alla rete Wi-Fi è una delle principali cause di accessi non autorizzati alla rete locale e, di conseguenza, a dati e informazioni potenzialmente sensibili;

  2. prediligere, ove possibile, l'utilizzo di sistemi di autenticazione a due fattori;

3. mantenere aggiornati sistemi operativi e software, sia desktop che mobile, utilizzati per svolgere la prestazione lavorativa: gli aggiornamenti sono importanti in quanto spesso risolvono falle di sicurezza sfruttabili per accedere ai dispositivi e ai dati in essi contenuti;

4. utilizzare e mantenere aggiornati specifici software antivirus e firewall, che offrono una tutela nei confronti dei rischi normalmente connessi alla navigazione in rete;

5. implementare sistemi di backup per assicurare la disponibilità di dati e informazioni in ogni momento, sia tramite sistemi cloud che tramite dispositivi di archiviazione di massa come hard disk portatili: l'accesso ai dati va protetto adeguatamente, magari servendosi di soluzioni crittografiche;

6. nel lavorare da casa è altresì importante attuare una serie di misure organizzative per svolgere le proprie mansioni in un ambiente lavorativo idoneo, come avere cura nell'impostare la propria postazione di lavoro, non lasciare incustoditi i dispositivi e non condividere informazioni riservate con i propri familiari;

7. il luogo di lavoro dovrebbe presentare caratteristiche ambientali che garantiscono riservatezza e un ambiente protetto, silenzioso e dotato di adeguati sistemi che garantiscano la connettività;

8. lo smart working dovrebbe essere vietato in luoghi come strutture ricettive, locali/spazi pubblici o aperti al pubblico; è fatto divieto di connettersi a reti pubbliche o private non proprie;

9. utilizzare una password che presenti caratteristiche di sicurezza (ad es. lunghezza almeno X caratteri, presenza di caratteri alfanumerici/speciali, contenuto non riconducibile alla persona)

11. per quanto riguarda riservatezza e la protezione dei dati degli interessati mettere in atto ogni misura per evitare interferenze con l'ambiente lavorativo, disconnettere gli apparati al termine della sessione di lavoro e archiviare in modo sicuro la documentazione cartacea;

12. non lasciare il dispositivo in luoghi incustoditi e riporre in un luogo chiuso al termine delle sezioni di lavoro

Le indicazioni sopra esposte valgono per qualsiasi tipo di concreta applicazione dello "smart working". Nel caso in cui tale modalità di svolgimento della prestazione lavorativa è messa in atto tramite l'utilizzo dei propri dispositivi personali tali indicazioni devono essere seguite con particolare rigore. Vanno altresì seguite nel caso in cui l'istituzione scolastica sia in grado di fornire ai propri dipendenti dei dispositivi scolastici opportunamente configurati secondo le misure minime di sicurezza ICT per la PA.